



**DEPARTMENT OF THE ARMY**  
HEADQUARTERS, 15TH REGIMENTAL SIGNAL BRIGADE  
FORT GORDON, GEORGIA 30905-5729

REPLY TO  
ATTENTION OF:

ATZH-TB

6 March 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy Letter 20: Use of Automation Information Systems (AIS)

1. References:

- a. AR 25-1, Army Knowledge Management and Information Technology, 15 Jul 05
- b. AR 25-2, Information Assurance, 14 Nov 03
- c. AR 380-5, Department of the Army Information Security Program, 29 Sep 00
- d. Memo, ATIM, subject: Transmission of TRADOC Operational Traffic, 23 Aug 05

2. In December 1987, Congress passed the Computer Security Act of 1987. In January 1988, that act became Public Law 100-23-5. The law set forth a statutory requirement that all users, supervisors, managers and commanders of automation information systems (AIS) receive initial and annual training in automation security. This same requirement is also regulatory under paragraph 3-2f(4), reference 1b above. The information contained in this memorandum fulfills the user training requirement of both PL 100-23-5 and AR 25-2.

3. Users will read this policy letter before requesting a new email account, provide security clearance documentation from DPS, and acknowledge understanding by signing a Computer User Agreement (Enclosure 1). IASOs will retain initial signed agreements within their respective areas until user outprocesses the organization. All personnel are required to reread this policy annually and update their Computer User Agreement. Supervisors, managers and commanders will ensure that all personnel under their supervision comply with this policy.

4. **Purpose of Information Systems Security.** Thousands of AIS operate in the US government processing classified and sensitive unclassified information. These systems are vulnerable to computer hackers, hostile intelligence agents, thieves, and individuals with malicious intent. The rapid increase in AIS over the past few years has made security a major issue concerning the safeguarding of systems and most important, the data they process. The Information Systems Security Program defines various threats to



our AIS and applies countermeasures. The program is designed to protect against the following types of threat:

- a. Espionage.
- b. Compromise or unauthorized manipulation of classified and sensitive unclassified information.
- c. Unintentional loss or malicious destruction of data files.
- d. Malicious or unintentional damage to or destruction of AIS hardware and software.
- e. Theft of hardware and software.
- f. Unauthorized use of software that may contain malicious programs (e.g. computer viruses, logic bombs, etc.)
- g. Unauthorized personal use of AIS.
- h. Natural disasters that would destroy AIS resources, database or otherwise interrupt AIS services.
- i. An authorized AIS user who is ignorant of security policies and procedures. (This is a significant threat to AIS).

#### **5. Personal Responsibility.**

a. If you are an AIS user, supervisor, manager or commander of AIS operations, you are required under the law to apply prescribed security policies and procedures. Failure to do so may subject you to disciplinary action and penalties under the law. Information systems security policies and procedures are found in Army regulations and USASC&FG supplements to those regulations, unit SOPs and in this document.

b. Before you begin operating an AIS, be sure you understand and comply with the security requirements of the system. Ask your Information Assurance Security Officer (IASO) if you have any questions.

c. You are responsible for compliance with the following automation security policies and procedures which are divided into four areas: procedural security, data security,

*“Voice of Victory!.....Faithful Service!”*



physical security and communications security. These policies and procedures are not all-inclusive; however, they constitute the minimum "do's and don'ts" of system operation.

d. You are responsible for invoking password-protected screen savers, screen locks on the workstation after 10 minutes of non-use or inactivity. Systems are loaded with this setting and must remain so IAW AR 25-2, para 3-3c(1)(l).

**6. Procedural Security.** Procedural security dictates how you operate and maintain your system. Users, supervisors, managers and commanders will:

a. Obtain an automation security briefing from your IASO before using AIS equipment for the first time. (This memorandum fulfills this requirement.)

b. Maintain AIS equipment with care (for example, use properly, keep clean). The processing environment must also be kept as clean as possible. Smoking is not allowed in areas where AIS operate.

c. Connect AIS to a surge suppressor or uninterruptible power supply (UPS) and not directly to a power outlet.

**d. Adhere to the following related to computer software.**

(1) Only approved and accredited software packages may be installed on AIS by your IASO; users are prohibited from installing software.

(2) Personal copies of software are prohibited in the workplace for use on government-owned equipment.

(3) Computer games are not authorized on computers.

(4) Honor software copyright restrictions. No unauthorized copies of copyright software may be made for office or personal use. Copyrighted software may not be borrowed or removed from the workplace.

(5) Copyrighted software will not be loaded on another AIS unless it is authorized in vendor agreements.

(6) Protect against disaster. Always have backup copies of data files ready to go.

*"Voice of Victory!.....Faithful Service!"*



Update backup copies of data files regularly.

**e. Adhere to the following related to computer hardware.**

(1) Any hardware you use must be accredited. As the user, you must maintain property accountability. You cannot install and use your own hardware at work. Any hardware purchased for your unit must meet Army accreditation standards and be accounted for properly.

(2) You may not connect a fax or modem to a system with a network connection.

(3) You must ensure that no additional equipment is attached to your AIS without the knowledge and permission of your IASO.

**f. Adhere to the following related to passwords.**

(1) Safeguard assigned user passwords. Do not reveal passwords to anyone, and do not store them in plain text on an AIS. You are responsible for anything that occurs on the network under your logon name and password. If you share your password and someone logs on as you and then hacks a web site or downloads a hacker tool, you could be held responsible.

(2) Fort Gordon policy requires passwords to be at least ten (10) digits long, including at least two (2) uppercase characters, two (2) lowercase characters, two (2) numbers, and two (2) special characters. Passwords are not to form a word or any part of your name. You may not tamper with your computer to avoid the Fort Gordon password policy. Passwords must be changed every 6 months on unclassified systems, and every 3 months on classified systems.

(3) Do not configure a shared directory without password protection. This would enable everyone with access to the shared computer to modify, delete or download your files.

(4) Passwords that do not conform to the above standards are vulnerable to password-cracking programs continually used by hackers. Most password-cracking programs compare passwords to words in dictionaries. If your password is made up of words or acronyms, the program unscrambles your password and gives the hacker access to your computer. Once hackers gain access to your computer, they have access to much of the DoD network. Password protection is essential. Examples of good passwords include:

*"Voice of Victory!.....Faithful Service!"*



ATZH-TB

SUBJECT: Policy Letter 20: Use of Automated Information Systems (AIS)

#?RU44porp  
GR23\$#fqny  
26ibd##1PP

(5) Report compromised passwords immediately to your IASO.

(6) Protect equipment. Keep food, drink and electrical appliances away from an AIS.

(7) Protect an unattended computer. Always log off or lock (press *Ctrl-Alt-Del* simultaneously, then select the "Lock Workstation" button) when leaving your computer unattended.

**g. Adhere to the following related to virus protection.**

(1) Ensure external media is scanned before opening any files on the media.

(2) Should any warning or message appear indicating that a virus has been detected on your computer, contact your IASO immediately.

(3) Periodically check your antivirus definition for a current date. If the shield in the system tray is not present, or has any type of symbol on it, contact your respective IASO. This could indicate a problem with the antivirus software and should be looked at immediately.

(4) As a government employee, you are authorized to install Symantec Antivirus software on your home computer. Download and install Antivirus software from <https://www.acert.1stiocmd.army.mil/antivirus>, using the "unmanaged" option. (NOTE: Set the Live Update feature to scan at least once a week. If you schedule Live Update for 1000 on Tuesday, set the scan to run at 1130 Tuesday. This will ensure you have the most current antivirus software running during weekly scans.) When you scan your computer for viruses, set your antivirus software to scan "all files." Also, be sure to scan all diskettes and CD-ROMs.

**h. Adhere to the following related to jokes, chain mail, virus hoaxes and other computer hoaxes.**

(1) The internet is constantly flooded with bogus information such as messages

*"Voice of Victory!.....Faithful Service!"*



about potentially damaging viruses, and notices that Bill Gates will send you money for forwarding email to others. While some real information may be mixed in with these hoaxes and legends, it is unlikely. If you receive this type of message, the best course of action is to delete them without reading them. The premise behind a hoax is that it will stimulate the reader to get emotionally involved by making the reader angry, afraid, or eager for money, and forward the message to everyone the reader knows or can reach through a Global Address List. That creates "chain mail," which in turn creates bottlenecks in our email and other network servers, slowing them down. Chain mail can even cause network servers to crash. Because of this threat to our systems, you are strictly forbidden to forward these types of messages to anyone but your IASO.

(2) Virus hoaxes are not real viruses, but they can be harder to get rid of than real viruses. Virus hoaxes and other email hoaxes take up space on email servers, use up network bandwidth and waste time. They usually take the form of email warnings sent to large numbers of people to warn them about nonexistent viruses. Before you forward warnings such as these to your IASO, read the Hoaxes and Scams page on the ACERT or Symantec web site. If you receive a warning and are not sure if it is real, DO NOT send it to everyone you know; contact your IASO.

(3) Report immediately any suspected computer misuse or suspicious activity to your IASO.

(4) Computers will be restarted daily to allow any updates to take effect.

(5) Computers will remain powered on and will only be turned off as directed by DOIM or your IASO.

**7. Data Security.** Always protect classified and sensitive unclassified information. Sensitive and mission critical information requires protection from disclosure, alteration and loss. Classified data products must be safeguarded (processed and stored) under the provisions of AR-380-5 Information Security Program. Users, supervisors, managers and commanders will:

- a. Protect data files. Establish and periodically review access privileges for each sensitive file.
- b. Protect data storage media by securing removable media.
- c. Not attempt to access any data on an AIS or computer network unless specifically authorized such access.

*"Voice of Victory!.....Faithful Service!"*



d. Label diskettes with the contents of the data stored on them (classified and unclassified) and the name of the application program used. Handle diskettes carefully to avoid damage. Do not write on a diskette with pencil or pen. The correct procedure for labeling a diskette is to write the classification and identification data on the label and then attach the label to the diskette.

(1) Label diskettes used for classified data with the highest classification of information contained on the diskette.

(2) Store classified and unclassified diskettes in jackets to protect from damage.

(3) Mark classified data output products at the top and bottom of the page with the proper classification and required caveats (AR 380-5).

(4) Do not process data that exceeds the accreditation sensitivity level of the AIS. If you are not sure, ask your IASO.

(5) Store classified and sensitive AIS data products in authorized security container as defined in AR 380-5.

(6) Dispose of disks containing sensitive information IAW AR 380-5.

(7) Do not allow any unauthorized personnel (i.e., student personnel) access to your system.

(8) If you suspect someone has tampered with your files or the data in them, report it immediately to your IASO

**8. Communications Security.** The following policies and procedures apply to AIS that are networked, including systems with TSACS (Terminal Server Access System) dial-up modem capability. Users, supervisors, managers and commanders will:

a. Use the email system only for transmission and receipt of unclassified, non sensitive, informal communications. There is a general attitude that "if it's not classified, we can send it over email." NOT TRUE! The email network is extremely vulnerable to wiretap and susceptible to intercept. Convenience does not justify transmitting sensitive information via email when it otherwise should be sent through encrypted channels.

b. Per reference 1d above, TRADOC activities will use the following guidance

*"Voice of Victory!.....Faithful Service!"*



regarding the classification and transmission of operational data: a. Data classified as "For Official Use Only" will, at a minimum, be signed using CAC/PKI.

(1) Data classified as "**Sensitive but Unclassified**" will, at a minimum, be signed and encrypted using CAC/PKI.

(2) Data classified as "**Confidential**" or "**Secret**" will be transmitted over a network with a minimum security classification of SECRET (e.g., SIPRNET, JWICS).

(3) **Unclassified Critical and Sensitive Operational traffic** will be transmitted over a secure network. For the purpose of this memorandum, **Unclassified Critical and Sensitive Operational traffic will include but not be limited to correspondence containing "shortfalls in training" due to funding, General Officer's Overseas Travel Schedules, and all deployed/deploying troop information**.

**9. Physical Security.** Physical security limits access to your processing environment and provides security for your AIS. AIS users and their supervisors must:

- a. Protect data processing areas. Recognize, politely challenge and assist people who do not belong in your area.
- b. Limit access to AIS. Know those who are authorized to use, service and repair your AIS. Use system lock-down or power switch locking devices when available.
- c. During nonduty hours and when offices are left unattended, lock doors to offices and rooms which house AIS equipment.
- d. Ensure that AIS hardware and software are handreceipted by serial numbers to designated handreceipt holders. Hardware and software must have an accountability chain back to the Property Book Officer.
- e. Challenge personnel carrying AIS components out of an office or building.
- f. Do not allow any AIS hardware to be moved from its accredited location without the knowledge and approval of the IASO. This includes turning in equipment for maintenance.

*"Voice of Victory!.....Faithful Service!"*



g. Restrict access to areas where classified information is being processed.

h. Do not allow storage media on which sensitive but unclassified data or applications have resided to leave controlled channels until the data has been appropriately destroyed.

**10. Personal Use of Government Computers.** There are detailed rules for appropriate and inappropriate use of government computers. There are rules governing how computers may be used for personal use. The United States government provides you a computer to do your assigned duties. The taxpayer is not required to provide you free and unlimited internet access. The rules are simple and clear. **Government computers are to be used by government employees only for official business, authorized personal use, and limited morale and welfare communications between deployed soldiers and their family members.**

a. Official business is that which is related to your official duties.

b. Authorized personal use is defined in the Joint Ethics Regulation (JER). Authorized personal use includes brief access and searches for information on the internet and sending short email messages.

c. The JER also requires commanders and supervisors to make every effort to ensure that personal use of government computers:

(1) Does not adversely affect the performance of official duties.

(2) Is of reasonable duration and frequency and, when possible, done during off duty hours.

(3) Serves a legitimate public interest, such as furthering the education and self improvement of employees, improving employee morale and welfare, or job searching in response to downsizing. Using government computers to send electronic mail (email) between deployed soldiers and their immediate family members is authorized.

d. Personal use of government computers must not overburden the communication system. Cruising the internet for personal or entertainment purposes is not authorized.

e. Personal use of government computers must not adversely reflect on DoD or DoD

*"Voice of Victory!.....Faithful Service!"*



components. The JER specifically prohibits using government computers for pornography, spam or chain mail, personal gain, or any action that violates another statute or regulation.

f. Other misuse of government computers includes: hacking or using hacking tools, visiting hacker web sites, deliberately installing viruses on DoD computers, trying to mask or hide identity, attempting to bypass security policy and using internet telephony, "streaming" audio/video web sites (e.g., keeping a web page open to receive hourly stock updates).

**11. Personal Liability for Fraud and Criminal Activity in Connection with Computers** (Ref Title 18, Section 1080, US Code). AIS users, supervisor, managers and commanders must be aware of the following:

a. Federal law provides for punishment to include a fine and imprisonment for any individuals who:

(1) Knowingly accesses a computer without authorization, or exceeds authorized access, and obtains information which requires protection against unauthorized disclosures (NOTE: The offense is for the access and not necessarily any disclosure).

(2) Intentionally, without authorization accesses a government computer and, in so doing, affects the use of the government's operation of the computer.

(3) Intentionally accesses a government computer without authorization, and alters, damages, or destroys information or prevents authorized use of the computer.

(4) Accesses a government computer without authorization, or exceeds authorized access and obtains anything of value.

b. The above prohibitions and punishments apply to mere attempts - even if unsuccessful - to commit the listed crimes. Multiple access or multiple attempts constitute multiple offenses for the purposes of determining punishment.

c. The authorized user of automation equipment is personally responsible, under the law, to apply prescribed security policies and procedures contained within this memorandum. This policy is punitive in nature. Violators are subject to adverse administrative action and punitive action under the Uniform Code of Military Justice and as otherwise provided by federal law.

*"Voice of Victory!.....Faithful Service!"*

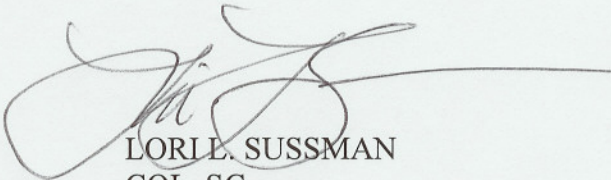


ATZH-TB

SUBJECT: Policy Letter 20: Use of Automated Information Systems (AIS)

**12. Acknowledgement.** Users, supervisors, managers and commanders will acknowledge by signature on the Computer User Agreement that they have read and understood the above instructions. Any questions regarding this memorandum must be answered by your respective IASO or Brigade IASO prior to signature. Personnel who refuse to acknowledge the briefing (this memorandum) will not be allowed to operate an AIS.

Encl  
Computer User  
Agreement



LORLE. SUSSMAN  
COL, SC  
Commanding

**DISTRIBUTION:**

Cdr, 15RSB  
Dean, 15RSB  
DBC, 15RSB  
CSM, 15RSB  
S1, 15RSB  
S2, 15RSB  
S3, 15RSB  
S4, 15RSB  
Cdr, 447<sup>th</sup>  
Cdr, 369<sup>th</sup>  
Cdr, 73<sup>rd</sup>  
Cdr, 551<sup>st</sup>  
Cdr, HHC, 15th RSB

*"Voice of Victory!.....Faithful Service!"*



# 15<sup>th</sup> RSB Computer User Agreement

## Section 1. User Information

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
LAST NAME FIRST MI RANK  
ORG: \_\_\_\_\_ PHONE: \_\_\_\_\_

## Section 2. User Obligations

Initials after each statement below indicates the user named above has read and agrees to abide by the obligations stated herein. By placing your initials in the area provided, you are agreeing to full compliance.

STATEMENT	INITIALS
1. User ID and password are sensitive but unclassified (SBU) and will be protected as such. I will NOT divulge my User ID and password to other individuals or sources. I accept full responsibility for all actions taken while logged onto the computer under my assigned User ID.	
2. I understand that I am responsible for invoking password-protected screen savers, screen locks, or other lockout features to automatically activate when my computer is inactive for <b>10 minutes</b> .	
3. I understand that all passwords that I create will be a minimum of 10 characters in length and will be comprised of 2 upper and 2 lower case letters, 2 numbers and 2 special characters. Words found in any dictionary, in any language, will not be used. I further understand that the life cycle of network level passwords will not exceed <b>180 days</b> .	
5. I understand that Administrator passwords are to be used only by appointed IASOs within 15 <sup>th</sup> RSB and are not to be circumvented or changed under any circumstances.	
6. I understand use for other than OFFICIAL US Government business, including use of email and Internet access for non-approved/non-Government purposes is not allowed and is a violation of federal law unless specifically allowed by other policies in place on the Installation.	
7. I understand that no games will be used on Government computers, this includes all Windows/DOS games supplied with those applications. I will notify my IASO to remove any games found.	
8. I understand that the initiation of, transmission of, or forwarding of such things as chain letters or other inappropriate broadcasts via email is prohibited. I further understand that I will immediately report the receipt of these types of emails to my IASO.	
9. I understand that I am not allowed to maintain adult material or visit sites that maintain and/or distribute adult material while using this account and DOD-owned hardware and software.	
10. I understand that storing, processing, or displaying offensive or obscene material, such as pornography, hate literature, etc. is prohibited.	
11. I understand any illegal, fraudulent or malicious activities are prohibited. These activities include but are not limited to: partisan political activity and political or religious lobbying or activities on behalf of organizations having no affiliation with the U.S. Army.	
12. I understand that activities for the purpose of personal or commercial financial gain are prohibited. These activities include but are not limited to: chain letters, solicitation of business or services, sales of personal property.	
13. I understand I am not allowed to annoy or harass another person, e.g., by sending uninvited email of a personal nature or by using lewd or offensive language.	
14. I understand that storing or processing classified information on any computer not explicitly approved for classified processing is prohibited.	
15. I will not allow or permit any unauthorized individuals to access a Government-owned computer. This includes, but is not limited to: allowing unauthorized individuals to add software/hardware or to perform any maintenance on my computer.	
16. I understand connecting to the network is subject to having all activities monitored and recorded without further notice. Any individual who uses this computer expressly consents to such monitoring and is advised that if this monitoring reveals possible evidence of unauthorized or criminal activity, this evidence may be provided to federal law enforcement officials for possible punishment/prosecution.	
17. I understand that NO "freeware" or "shareware" software, including trial versions offered by vendors, will be installed on any Government-owned computer without written authorization and approval from the DAA (Installation Commander). I further understand that all requests to install "freeware" or "shareware" software, including trial versions, must be coordinated through Brigade Automation and the Brigade Commander to the DAA (Installation Commander).	
18. I understand that I must have the most current anti-virus software installed and running at all times and will periodically review my antivirus configuration for current definitions.	
19. I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.	
20. I know I am subject to disciplinary action for any abuse of access privileges.	

## Section 3. User Validation

I understand and agree to abide by the guidelines listed above.

SIGNATURE: \_\_\_\_\_ DATE: \_\_\_\_\_

UPDATED SIGNATURE: \_\_\_\_\_ DATE: \_\_\_\_\_

UPDATED SIGNATURE: \_\_\_\_\_ DATE: \_\_\_\_\_